Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 07 June 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The New York Daily News reports that explosions inside a chemical storage plant on Staten Island killed a man and sent many others running for safety. (See item 2)

- Dow Jones reports Citigroup Inc.'s CitiFinancial lending unit said a box of computer tapes containing its client's personal account and payment history information were lost while being shipped to a credit bureau through a third party. (See item 3)

- WNEP reports residents in Monroe County, Pennsylvania, have been told not to drink, shower or even wash their dishes with their water, due to pollution from a petroleum−based substance. (See item 19)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 06, Associated Press* — **Severe thunderstorms cause large power outage.** More than 110,000 homes and businesses remained without power Monday, June 6, after severe thunderstorms swept across Michigan, officials said. Hundreds of power lines remained on the ground in the state overnight, creating a danger in many areas, Consumers Energy Co. spokesperson Kevin Keane warned. As of 7:30 a.m., about 30,000 Consumers Energy customers were without service, down from the 84,000 affected by the storms on Sunday, June

5, Keane said. In addition, about 83,000 DTE Energy customers in southeastern Michigan remained blacked out Monday morning, utility spokesperson Michael Porter said. It would take until late Tuesday, June 7, to finish restoring service, he said. In all, some 103,000 DTE customers lost service. Wind gusting to 91 mph left at least 50,000 customers without power in Indiana, though most had service restored by Monday morning.
Source: http://abcnews.go.com/US/wireStory?id=823797

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *June 04, New York Daily News* — **Explosion at Staten Island chemical storage plant kills one person.** Explosions inside a chemical storage plant in Staten Island, NY killed a man and sent neighbors running for cover Friday afternoon, June 3. Fire officials were investigating what sparked the deadly blaze in the brick building in an industrial area. More than 110 firefighters spent three hours extinguishing the blaze, which broke out inside Plating System Inc. around 2:13 p.m. (EDT), officials said. An unidentified man, who neighbors believed was repairing a leaking fuel tank, was killed. Five firefighters suffered minor injuries, officials said. The plant was in violation of several city laws, including storing more than 10 times the acceptable amount of flammable methanol, said Charles Sturcken of the city Department of Environmental Protection.
Source: http://www.nydailynews.com/news/local/story/315738p−270173c. html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *June 06, Dow Jones Newswires* — **CitiFinancial customer data lost while in transit.** Citigroup Inc.'s CitiFinancial lending unit said a box of computer tapes containing its client's personal account and payment history information were lost while being shipped to a credit bureau through a third party. Consumer finance unit CitiFinancial also disclosed the breach in a letter sent to its 3.9 million branch network customers. The tapes contained names, social security, numbers, account numbers and personal history of customers in the U.S. as well as customers from closed accounts from CitiFinancial. In a press release Monday, June 6, CitiFinancial said it doesn't believe the lost data was used inappropriately and said it so far hasn't received any reports of unauthorized activity. CitiFinancial said there is little risk of the accounts being compromised because customers already received their loans.
Source: http://money.iwon.com/jsp/nw/nwdt_rt_top.jsp?cat=TOPBIZ&src=704&feed=dji&section=news&news_id=dji−00043420050606&date=20050606&alias=/alias/money/cm/nw

4. *June 06, Reuters* — **Bombs found at U.S. companies in Argentina.** Argentine police found small bombs on Monday, June 6, at outlets of three different U.S.−based companies in or near Buenos Aires, one of which exploded without causing any injuries. A small homemade bomb went off in a Blockbuster Inc. video store just outside the capital overnight, causing minor damage to windows, a police official said. Bombs were also found at a McDonald's Corp. restaurant and Citibank branch but police bomb squads removed them without causing any damage. Police found pamphlets at the bomb sites signed by the "Mariano Moreno National Liberation Commando," which said "our aim is to liberate (Argentina) from imperialism." Last year, the Argentine capital and provinces were hit by a string of similar bomb attacks, mainly targeting banks. Anti−U.S. slogans and U.S. flag burnings are common at Argentine protests of unemployed workers or leftists, who blame foreign multinationals and Washington's economic influence for the country's economic troubles.
Source: http://abcnews.go.com/US/wireStory?id=823788

5. *June 06, Associated Press* — **Professor charged with identity theft.** A community college professor has been charged with using his students' names and Social Security numbers to obtain department store credit cards. Bradley Neil Slosberg, of Winter Haven, FL, was arrested Friday, June 3, on charges of criminal use of personal identification and scheming to defraud, the Polk County, FL, Sheriff's Office said. Slosberg and his girlfriend, Deborah Hafner, stole the identities of at least three of the students from his anatomy and physiology class at Polk Community College, sheriff's office spokesperson Carrie Rodgers said. Hafner filled out the credit card applications and committed the forgeries, Rodgers said. Slosberg had asked his students to write their names and Social Security numbers on a sign−in sheet, students said.
Source: http://abcnews.go.com/US/LegalCenter/wireStory?id=822816

6. *June 06, Government Accountability Office* — **GAO−05−412: USA Patriot Act: Additional Guidance Could Improve Implementation of Regulations Related to Customer Identification and Information Sharing Procedures (Report).** Title III of the USA Patriot Act of 2001, passed after the September 11 terrorist attacks, amended U.S. anti−money laundering laws and imposed new requirements on financial institutions. Section 326 of the act required the development of minimum standards for verifying the identity of financial institution customers. Section 314 required the development of regulations encouraging the further sharing of information between law enforcement agencies and the financial industry and between the institutions themselves. Because of concerns about the implementation of these new provisions, the Government Accountability Office (GAO) determined how (1) the government developed the regulations, educated the financial industry on them, and challenges it encountered; (2) regulators have updated guidance, trained examiners, and examined firms for compliance; and (3) the new regulations have affected law enforcement investigations. To help financial institutions implement their Customer Identification Programs (CIPs), GAO recommends that Treasury, through its Financial Crimes Enforcement Network (FinCEN) and with the federal financial regulators and self−regulatory organizations, develop additional guidance on ongoing implementation issues. To improve examinations of compliance with CIP, GAO also recommends that FinCEN work with the federal financial regulators to develop additional guidance for examiners. Treasury agreed with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d05412high.pdf
Source: http://www.gao.gov/new.items/d05412.pdf

7. *June 04, Associated Press* — **Hackers break into health system's Websites.** About 14,500 users of various Duke University Health System Websites were told to find new passwords after the system's operators discovered a security breach. Computer hackers did not gain access to any patient information or financial information such as credit card numbers, said Asif Ahmad, chief information officer for Duke's medical center and health system. However, in about 9,000 cases, four or six digits of users' nine−digit Social Security numbers were exposed. Duke officials believe nobody lost enough data to become a victim of identity theft. Starting Friday, June 3, Duke sent e−mails to everyone using the Websites, explaining the problem. A system administrator uncovered the tampering during a routine check of activity about 4:30 p.m. May 26, more than 12 hours after it apparently occurred. "Unfortunately we were going into the Memorial Day holiday weekend," Ahmad said. That complicated the process of contacting the heads of all affected department and ferreting out the hackers' impact, he said.
Source: http://www.wral.com/news/4569493/detail.html?rss=ral&psp=new s

8. *June 03, TechWeb News* — **Phishers targeting smaller entities.** Phishers are taking aim at ever−smaller financial targets, an association of technology companies said Friday, June 3, in its monthly report on the e−scams and schemes. According to the Anti−Phishing Working Group (APWG), a collection of over 1,400 companies, banks, ISPs, and government agencies, April saw a large increase in the number of credit unions targets by phishers. Both relatively large regional credit unions to niche institutions that serve narrow groups of workers were targeted, said the APWG. "Hackers are modifying their attack methods by shifting away from attacking popular or large institutions," said the APWG in its report. There's also evidence that phishers are cooperating, said the APWG, which noticed several occasions in April when multiple attacks were launched simultaneously at the same target. "This points to a common root, or −− at least −− some interconnection and organization among phishers," concluded the report.
Anti−Phishing Working Group April Report:
http://antiphishing.org/APWG_Phishing_Activity_Report_April_ 2005.pdf
Source: http://www.techweb.com/wire/security/164300203

9. *June 03, Financial Crimes Enforcement Network* — **Dealers in precious metals, stones or jewels required to establish anti−money laundering programs.** Under an interim final rule announced on Friday, June 3, by the Financial Crimes Enforcement Network (FinCEN), dealers in precious metals, stones or jewels are required to establish anti−money laundering programs. At a minimum, dealers must establish an anti−money laundering program that comprises the following four elements: Policies, procedures and internal controls, based on the dealer's assessment of the money laundering and terrorist financing risk associated with its business; A compliance officer who is responsible for ensuring that the program is implemented effectively; Ongoing training of appropriate persons concerning their responsibilities under the program; and Independent testing to monitor and maintain an adequate program. FinCEN is issuing this regulation to better protect those that deal in jewels, precious metals and precious stones from potential abuse by criminals and terrorists. "The characteristics of jewels, precious metals and precious stones that make them valuable also make them potentially vulnerable to those seeking to launder money," said William J. Fox, Director of FinCEN.
Interim Final Rule: http://www.fincen.gov/antimoneylaundering060305.pdf
Source: http://www.fincen.gov/nr060305.pdf

[Return to top]

Transportation and Border Security Sector

10. *June 06, Agence France−Presse* — **British Airways tries new scheme to track luggage.** British Airways (BA) is testing tiny radio transmitters on passengers' luggage in order to prevent suitcases going astray and save the industry hundreds of million of dollars annually, officials said Saturday, June 4. Check−in staff have until now fitted stickers with barcodes to every item of luggage which can be scanned as they are routed along conveyor belts, but the system breaks down if the stickers are torn, bent or ripped off, they said. BA said it believes the Radio Frequency Identification (RFID) scheme would ensure that virtually all travelers receive their baggage at destination. BA said some 18 per 1,000 bags on its flights are misplaced.
Source: http://www.usatoday.com/travel/news/2005−06−06−luggage−trans mitters_x.htm

11. *June 06, Agence France−Presse* — **Door torn off United Airlines plane at Taiwan airport.** The side door of a United Airlines Boeing 777 aircraft was torn off Monday, June 6, when it suddenly moved away from a passenger gantry at Taiwan's Chiang Kai−shek airport, airport officials said. None of the 143 passengers and 11 crew on the plane, bound for Nagoya, Japan, were injured. "It was probably a communication problem," an airport official said.
Source: http://www.usatoday.com/travel/news/2005−06−06−united−door_x .htm

12. *June 06, New York Times* — **United Airlines approved for in−flight Internet service.** United Airlines is the first domestic airline to receive approval from regulators to install wireless Internet (Wi−Fi) networks on its planes. The airline is still at least a year away from having its in−flight Wi−Fi service up and running. When it does, sometime in mid− to late 2006, passengers will be able to check e−mail, send instant messages and surf the Web at 30,000 feet. Wi−Fi is also available in terminals across the country. Many airports, like LaGuardia in New York, charge a flat daily rate to use a wireless Internet connection, while JetBlue Airways offers free Wi−Fi at some of its gates. Dennis Cary, United's senior vice president for marketing, said the airline would charge for the in−flight service but had not yet determined what the cost would be. United's Wi−Fi system will piggyback on its existing onboard phone network, which is operated in a partnership with Verizon. Data will be transmitted to and received from the planes through towers on the ground.
Source: http://www.nytimes.com/2005/06/06/technology/06united.html?o ref=login

13. *June 06, Associated Press* — **United seeks to extend reorganization plan deadline.** UAL Corp., parent of United Airlines, has asked the judge overseeing its bankruptcy case for permission to extend the exclusivity period covering its reorganization to September. The exclusivity period, a part of bankruptcy law, prevents the submission of rival reorganization plans while a company works through its case. Though there are no known groups working on their own plans, such requests for such extensions are common practice in UAL's case. In court documents, the nation's second−largest carrier said it has largely finished restructuring its labor costs, but more work on plane leases and additional time to finalize its business plan is necessary.
Source: http://www.usatoday.com/travel/news/2005−06−06−united−bankru ptcy_x.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

14. *June 06, Agence France Presse* — **Japan discovers twentieth case of mad cow disease.** Japan said it has found its 20th case of mad cow disease. The health ministry confirmed Monday, June 6, that a 57−month−old Holstein cow in the northern island of Hokkaido had mad cow disease or bovine spongiform encephalopathy (BSE). Japan is the only Asian country to have confirmed cases of BSE. Its first case was discovered in September 2001.
Source: http://news.yahoo.com/s/afp/20050606/hl_afp/healthjapanmadco wus_050606102807

[Return to top]

Food Sector

15. *June 05, Oregonian* — **Fish imported with fungicide.** Canadian farmed salmon containing a banned fungicide was sold in the U.S. earlier this year. Stolt Sea Farm, part of the world's largest salmon farming company, said this week that 80,000 pounds of farmed chinook salmon from British Columbia with low levels of malachite green reached consumers in the U.S., Canada, China, Japan, and other Asian nations. Authorities in Canada said at least half went to the U.S. Malachite green is a fabric dye banned for use on food in the U.S. since 1991 and suspected of causing cancer.
Source: http://www.oregonlive.com/business/oregonian/index.ssf?/base /business/1117879024162450.xml&coll=7

16. *June 03, Food and Drug Administration* — **FDA works to trace source of foodborne illness in Florida.** The U.S. Food and Drug Administration (FDA) is initiating an investigation to determine the source of several clusters of a gastrointestinal illness known as cyclosporiasis that is associated with fresh basil served in Florida during mid−March through mid−April. Known as a traceback, the investigation will work to locate the source of the contaminated produce. The Florida Department of Health asked FDA on June 2, 2005, to begin the traceback after results of an epidemiological investigation implicated fresh basil as the source of illness in Florida. The Florida Department of Health has 293 laboratory−confirmed cases in 32 Florida counties during March and April of this year. The outbreak includes several clusters and a large number of sporadic cases. Cyclosporiasis is caused by the ingestion of the Cyclospora parasite and results in the infection of the small intestine. It causes diarrhea. Other symptoms include loss of appetite, substantial weight loss, stomach cramps, nausea, vomiting, muscle aches, low−grade fever, and fatigue. Cyclospora infection can be treated with appropriate antibiotic therapy.
Source: http://www.fda.gov/bbs/topics/NEWS/2005/NEW01183.html

17.

June 02, U.S. Department of Agriculture — **Lebanon reopens markets for U.S. beef products.** The U.S. Department of Agriculture (USDA) Thursday, June 2, announced that Lebanon has resumed the import of U.S. beef and beef products from animals under 30 months of age. In 2003, the U.S. exported $643,000 worth of beef and beef products to Lebanon. It is the third country in the Middle East region to reopen its market to U.S. beef. In 2003, the U.S. exported approximately $7.5 billion worth of beef, beef products, cattle and other ruminants and ruminant by−products. After the discovery of a cow infected with mad cow disease in the U.S., $4.8 billion worth of beef exports were banned. To date, USDA estimates that it has recovered $1.9 billion of the banned amount.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2005/06/0194.xml

[Return to top]

Water Sector

18. *June 06, Business Wire* — **Aging U.S. water infrastructure requires increased government spending, report says.** With water becoming a scarce commodity, the aging U.S. water infrastructure is a cause for much concern, new analysis from Frost & Sullivan reports. Although government spending in this sector is substantial, the infrastructure requires urgent restoration for compliance with updated water safety standards. What remains is a gap between budgeted and required investments. Remedial action on this front will give water equipment companies the necessary impetus to grow at a faster rate. The municipal water sector accounts for 40 percent of the total water usage in the Unites States. "Water, a basic necessity, is turning out to be an investment necessity," notes Frost & Sullivan Research Analyst Santosh K. Ejanthkar. "The Environmental Protection Agency (EPA) estimates that heavy investments will be required in the U.S. to upgrade or replace the water infrastructure to ensure compliance with the safety standards prescribed by the Safe Drinking Water Act." In order for water equipment manufacturers to take advantage of the increasing opportunities in the municipal water treatment and distribution sector, they must develop new technologies to treat emerging contaminants, the report states.
Report information: http://www.frost.com/prod/servlet/report−homepage.pag?repid=F255−01−00−00−00&ctxst=FcmCtx1&ctxht=FcmCtx2&ctxhl=FcmCtx3&ctxixpLink=FcmCtx4&ctxixpLabel=FcmCtx5
Source: http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20050606005470&newsLang=en

19. *June 05, WNEP News (PA)* — **Water contaminants identified in Monroe County, Pennsylvania.** Sunday, June 5, was the third day without water for about 10,000 people in Monroe County, PA. The residents have been told not to drink, shower or even wash their dishes with their water. Officials from Pennsylvania American Water Company said the water is polluted with a petroleum−based substance. At the community's water treatment plant, Pennsylvania American has drums full of chemicals used to treat water. They said one of those drums was contaminated. The water company and the state Department of Environmental Protection expect test results back Monday morning, June 6, and don't know when the water will be usable. The water company is asking residents to run their hot and cold water for about 15 minutes to help flush out the system.

Source: http://www.wnep.com/global/story.asp?s=3433894&ClientType=Pr intable

[Return to top]

Public Health Sector

20. *June 06, Anchorage Daily News (AK)* — **Anchorage has new station for traveler quarantine.** Large numbers of international flights arriving in Anchorage, AK, have prompted the U.S. Centers for Disease Control and Prevention (CDC) to open a new quarantine station there to screen travelers for infectious diseases. "We try to select those airports that provided us the largest percentage of the arriving international traffic," said Marty Remis, deputy branch chief with the CDC's Quarantine and Border Health Services branch. "And Anchorage fell into that group." The quarantine station will open in July. Most quarantine stations nationwide are in airports, and CDC officials hope to open the Anchorage site there. The airport used to house a station that closed about two decades ago, said Linda Close, marketing director for Ted Stevens Anchorage International Airport. Achorage's new facility will boost the CDC's presence on the West Coast, said Ram Koppaka, acting chief of the CDC's Quarantine and Border Health Services branch. Stations exist or will open in Honolulu, Seattle, San Francisco, Los Angeles, and San Diego, he said.
Source: http://www.adn.com/news/alaska/story/6576296p−6459632c.html

21. *June 06, Chemical & Engineering News* — **New route found to tuberculosis drug resistance.** The three−dimensional structure of a protein manufactured by Mycobacterium tuberculosis suggests a new strategy by which the tuberculosis−causing organism may be able to outmaneuver fluoroquinolone antibiotics. These drugs kill bacteria by interfering with DNA gyrase, a DNA−binding enzyme that prevents the bacterium's genomic DNA from becoming tangled during replication. Fluoroquinolones bind to the DNA−bound gyrase and prevent the enzyme from doing its work. But resistance to these important antibiotics is on the rise, notes David Hooper, an infectious diseases expert at Massachusetts General Hospital. So far, nearly all fluoroquinolone−resistant M. tuberculosis strains outsmart fluoroquinolones by just one mechanism: They can make a modified DNA gyrase that isn't susceptible to the antibiotics. Recently, fluoroquinolone resistance also has been observed in other disease−causing bacteria. Instead of making a modified DNA gyrase, however, these bacteria produce a small protein that protects DNA gyrase from inhibition by fluoroquinolone. Such strains are worrisome because the genetic instructions for making the protective protein are contained in a DNA plasmid that can be passed rapidly from one bacterium to another, notes John Blanchard of Albert Einstein College of Medicine. M. tuberculosis bacteria make a similar protective protein, named MfpA, according to Blanchard. The similarity to DNA has led Blanchard's team to suggest that MfpA and its relatives interact directly with DNA gyrase.
Source: http://pubs.acs.org/cen/news/83/i23/8323notw4.html

22. *June 05, Public Health Agency of Canada* — **New Ebola, Marburg vaccines effective in animal models.** Scientists from the Public Health Agency of Canada (PHAC) −− with assistance from the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) −− have developed vaccines against the Ebola and Marburg viruses that have been shown to be effective in non−human primates. Canadian researchers Heinz Feldmann and Steven Jones of PHAC's National Microbiology Laboratory and Thomas Geisbert of USAMRIID report that the

vaccines have proven 100 percent effective in protecting monkeys against infection from these viruses. Monkeys are known to develop hemorrhagic fever symptoms that are similar to those observed in humans infected by these viruses. Demonstrating that these vaccines are safe and effective in monkeys is a promising indicator of their real potential for use in humans. According to Geisbert, this is the first vaccine system, or platform, that has protected nonhuman primates from both Ebola and Marburg. “In addition, the vaccine targets dendritic cells, which are the same cells that Ebola and Marburg attack,” said Geisbert. “These cells are also important in generating a protective immune response. So the vaccine goes exactly where we want it to go."
Source: http://www.phac−aspc.gc.ca/media/nr−rp/2005/2005_21_e.html

23. *June 05, USA Today* — **Quick action may head off global epidemic.** After poring over old medical records, studying census data and cranking out mathematical models, scientists and health officials are beginning to believe they have a chance to stop a bird flu pandemic before it kills millions of people worldwide. The key: detecting an outbreak early and rushing powerful antiviral drugs to the source to throttle a pandemic at birth before it can break out of Southeast Asia, carrying sickness and death around the globe. "It is the first time in the history of mankind that anyone has thought about keeping a worldwide pandemic at bay," says William Aldis, the top World Health Organization (WHO) official in Thailand. But the window of opportunity could close quickly, and the world is not yet prepared to take advantage of it, researchers say. Rich countries are stockpiling antiviral drugs, but there is little available in the impoverished backwaters of Southeast Asia where an outbreak is likely to begin. Avian influenza, an infectious disease of birds caused by type A strains of the influenza virus, jumped to humans in 2003. The H5N1 strain that has infected people has killed 54 of the 98 people infected, a 55 percent death rate.
Source: http://www.usatoday.com/news/health/2005−06−05−bird−flu−cove r_x.htm

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

24. *June 06, Federal Computer Week* — **Interoperability explored by DHS using encryption software.** The Department of Homeland Security (DHS) plans to make an announcement this week in Dallas, TX, about the implementation of new software that lets existing and new communications equipment interoperate securely. The new protocol is designed to overcome the communications difficulties that plagued first responders during the September 11, 2001, terrorist attacks. Police, firefighters and other first responders were often unable to communicate because of differences in the equipment they used, which contributed to the deaths of some firefighters in the World Trade Center. The Cryptographic Overlay Mesh Protocol (COMP) allows radios, mobile phones, laptop computers and other equipment to communicate with one another, said Mark Tucker, chief executive officer the company which

developed the protocol. COMP connects land−based telephone lines, radio systems, wireless networks, satellite transmissions, peer−to−peer networks and mobile phone systems, Tucker said. Through proxy programs, it is also "100 percent backward−compatible, back to analog," he said. The Dallas Love Field Wireless Integration Project will connect all law enforcement agents and first responders who cover the city's airport. The project will serve as a model for eventual statewide and national adoption of the technology.
Source: http://www.fcw.com/article89082−06−06−05−Print

25. *June 06, Orlando Sentinel* — **Florida beach drill will test disaster response.** More than 200 emergency personnel from local, state and federal agencies are expected to participate in a mock terrorism drill in Daytona Beach Shores, FL, Tuesday, June 6, to practice responding to a plane crash. About 34 agencies will participate in the $38,000 drill, which was funded by a grant from the U.S. Department of Homeland Security's Office for Domestic Preparedness. The drill is designed to simulate a terrorist attack on an MD−88 aircraft that has just taken off from Daytona Beach International Airport, Mauney said. During the scenario, the plane is struck by missiles as it ascends 300 to 500 feet. As the plane goes down, it clips a hotel before crashing into the Atlantic Ocean. Of the 109 passengers on board, 20 die on impact, and 89 are left fighting for their lives in the water. Emergency crews will pull people and mannequins from the plane and surf and will rescue three people from the elementary school. The Coast Guard will also pull mannequins from the ocean. All victims will be taken to hospitals around the county.
Source: http://www.news−journalonline.com/NewsJournalOnline/News/Local/03AreaEAST01060605.htm

26. *June 05, Desert Dispatch (CA)* — **Drill tests comprehensive pre−plan.** During a fire drill Saturday, June 4, in Apple Valley, CA, Fire Protection District firefighters practiced using the recently created Ord Mountain Wildlands Fire Pre−plan, a comprehensive overview of the area intended to minimize the impact of possible wildfires. The pre−plan is based on an elaborate collection of intelligence gathered on the area. The department has binders with information on each of the 22 sectors that would be given to task force leaders in the event of a fire in the area. Aerial photos, topographic maps, locations and types of fire hydrants are included. "It tells the leader what to expect when he goes to that area and he can base his objectives on that pre−plan," Captain Kenny Sanders said. Citizens with the Community Emergency Response Team and the Friends of Animals During Disasters were stationed at a different command post and went into the field to simulate their roles. An evaluative lunch was planned at the end of the drill so participants could point out the strengths and weaknesses of the plan.
Source: http://www.desertdispatch.com/2005/111798821744073.html

27. *June 05, The Boston Globe (MA)* — **Terror response is tested at Logan Airport.** Authorities at Logan International Airport, in Boston, MA, conducted a terror response drill, "Operation Atlas," on Saturday, June 4. Eight months in the planning and at a cost $750,000 in federal funds, it was one of the largest of its kind, designed to test emergency coordination plans, give a clearer picture of what still needed improvement, and allow personnel at scores of agencies to get to know each other and work as a team, essential in a real emergency. More than 50 federal, state, and local agencies from San Francisco to Paris worked with United Airlines, others in the private sector, and the military. A United plane and flight crew, along with 80 volunteer passengers, spent two hours in the air. Officials pinpointed several areas that could be improved. Massachusetts Port Authority Fire Chief Robert J. Donahue said training and

casualty processing needed improvements, and both he and Boccia said agency heads need a better way to communicate. A full analysis will not be available for another five to six weeks, Boccia said. Officials said they took lessons learned during the notorious shoe−bomb incident, which forced a Miami−bound plane from Paris to land in Boston, as well as during last summer's Democratic National Convention, and applied them during Operation Atlas.
Source: http://www.boston.com/news/local/massachusetts/articles/2005/06/05/terror_response_is_tested_at_logan/

[Return to top]

Information Technology and Telecommunications Sector

28. *June 06, Government Computer News* — **Department of State to promote cybersecurity awareness.** June is designated as the Department of State's Cybersecurity Awareness Month. Between June 7 and June 29, the Diplomatic Security Bureau's Computer Security Office and the Information Resources Management Bureau's Information Assurance Office will sponsor the project to improve employees' understanding of proper security procedures. The bureaus plan to hold events that will include topics on how to fend off phishing scams and other security risks based on social engineering, a demonstration of how hackers work, explanations of how to become a certified IT professional and information on spyware, antivirus software and other tools. The sessions will feature speakers from the National Security Agency, the FBI, the Agency for International Development and leading technology companies.
Source: http://www.gcn.com/vol1_no1/daily−updates/35993−1.html

29. *June 04, eWeek* — **Anti−virus companies warn of Trojan attack that builds botnets.** Anti−virus researchers are sounding the alert for a massive, well−coordinated hacker attack using three different Trojans to hijack PCs and create botnets−for−hire. The three−pronged attack is being described as "unprecedented" because of the way the Trojans communicate with each other to infect a machine, disable anti−virus software and leave a back door open for future malicious use. Roger Thompson, director of malicious content research at Computer Associates International Inc. said that this attack "… clearly points to a very well−organized group either replenishing existing botnets or creating new ones." Once the three Trojans are installed, the infected computer becomes part of a botnet and can be used in spam runs, distributed denial−of−service attacks or to log keystrokes and steal sensitive personal information. According to CA's Thompson, the success of the three−pronged attack could signal the end of signature−based virus protection if Trojans immediately disable all means of protection. He said he thinks the attack, which used virus code from the Bagle family, is the work of a very small group of organized criminals. With the rapid proliferation of new types of virus, Trojan and worm attacks, PC users are urged to be strict about following security guidance.
Source: http://www.eweek.com/article2/0,1759,1823633,00.asp

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures. **US−CERT Operations Center Synopsis:** US−CERT reports a heap−based buffer overflow that affects the PHP 'pack()' function call. An attacker that has the ability to make the PHP interpreter run a malicious script may exploit this condition to execute arbitrary instructions in the context of the vulnerable process. This function allows a malicious programmer to set references to entries of a variable hash that have already been freed. This can lead to remote memory corruption and may allow them to gain access to potentially sensitive information, such as database credentials.

Current Port Attacks

Top 10 Target Ports	135 (epmap), 445 (microsoft−ds), 1026 (−−−), 1027 (icq), 1433 (ms−sql−s), 1434 (ms−sql−m), 4899 (radmin), 139 (netbios−ssn), 1028 (−−−), 25 (smtp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

30. *June 06, Government Technology* — **Kentucky state parks get wireless Internet access.** Last fall, the Kentucky Department of Parks rolled out a pilot project to provide free wireless Internet access in guest rooms at Lake Barkley and Rough River Dam state resort parks. Guests may now easily get to the Internet using either the network card built into their laptops or by borrowing a device that provides that access. "We're seeing a lot of people traveling for pleasure who are so used to having an Internet connection wherever they go, so this is a potential draw for vacationers," said Sharon Roark, director of the technology division. The department now plans to expand wireless access to all of the remaining 15 resort parks. Plus wireless access will extend beyond guest rooms to conference rooms and lodge lobbies, Roark noted. Wireless access is expected to be available in all parks by year's end.
Source: http://www.govtech.net/news/news.php?id=94186

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.